TennCare

Companion Guides

(TCCGs)

Front Matter

Version 4010A1

October 2008 Version 2

Disclaimer: TennCare Companion Guides (TCCGs) are intended to be technical documents describing the specific technical and procedural requirements for interfaces between TennCare and its trading partners. TCCGs do not supersede either the Managed Care Contractors (MCCs) contracts or the specific procedure manuals for various operational processes. Where there are conflicts between TCCGs and either the MCC contracts or operational procedure manuals, the contract or procedure manual will prevail. Substantial effort has been taken to minimize any such conflicts or errors; however, TennCare or its employees will not be liable or responsible for any errors or expenses resulting from the use of information in these documents. If you believe there is an error in any document, please notify the TennCare Information Systems Division immediately.

Table of Contents

Article I. Introduction

Section 1.01 Document Objective

This Companion Document provides information related to the HIPAA Transactions, as well as the other ways in which health plans and program contractors will receive information from the TennCare administration via various supplemental files.

Section 1.02 Companion Guide Organization

TCCGs are organized into multiple documents that are available on the TennCare HIPAA website. Each HIPAA implementation guide has at least one associated TCCG available on the website (http://tennessee.gov/tenncare/pro-edi.html or http://www.state.tn.us/tenncare/pro-edi.html). This distributed documentation method allows each TennCare Business Associate to access and download only the transactions that apply to their line of business instead of downloading all the TCCGs .

The following TCCG Documents are available.

- 270 Eligibility Verification Transaction (pdf)
- 270 TennCare Outbound Eligibility Verification Transaction (pdf)
- 271 Eligibility Response Transaction (pdf)
- 271 TennCare Inbound Eligibility Response Transaction (pdf)
- 271 Unsolicited Transaction (MCC 834 limitations file) (pdf)
- 271U Service Limits Overview Document (pdf)
- 271U Service Limits BHO (pdf)
- 271U Unsolicited Companion Guide BHO (pdf)
- 276 Claims Status Request Transaction (pdf)
- 277 Claims Status Response Transaction (pdf)
- 278 Prior Authorization (Services Review) Request Transaction (pdf)
- 278 Prior Authorization (Services Review) Response Transaction (pdf)
- 820 Capitation (Premium Payment) Transaction (pdf)
- 834 Enrollment and Audit Transaction (pdf)
- 834 2300 Loop Definitions (pdf)

- 835 Electronic FFS Claims Remittance Advice Transaction (pdf)
- 837D Dental Claims/Encounter Transaction (pdf)
- 837I Institutional Claims/Encounter Transaction (pdf)
- 837P Professional Claims/Encounter Transaction (pdf)
- NCPDP Batch 1.1 Encounter Transaction (pdf)
- TennCare Trading Partner Agreement (Legal terms, EDI Form, Security Form) (pdf) Agreements are subject to change and users should contact TennCare for questions regarding revised versions.
- TennCare TCMIS Security/Information Request Form (pdf)
- Taxonomy Crosswalk (pdf)
- Local Codes Crosswalk (pdf)

Section 1.03 Relationship to HIPAA Implementation Guides

TCCGs are intended to supplement the HIPAA Implementation Guides (IGs) for each HIPAA transaction set. The rules for the formats, contents, and field values can be found in the Implementation Guides. TCCGs describe the technical interface environment with TennCare, including connectivity requirements and protocols, and electronic interchange procedures. TCCGs also provide specific information on the fields and values required for transactions sent to or received from TennCare.

TCCGs are intended to be supplemental to and NOT a replacement for the standard Implementation Guide for each transaction set*. Based upon reporting circumstances, certain loops or data elements that are normally situational may become required. Some of these situational loops may not be included within the* TCCG *for a given transaction; however, requirements within IGs must be followed when using different loops, segments and data elements. HIPAA required information must be met even if it's not part of the TCCG.*

The information in the TennCare documents is not intended to:

- Modify the definition, data condition, or use of any data element or segment in the standard Implementation Guides.
- Add any additional data elements or segments to the defined data set.
- Utilize any code or data values that are not valid in the standard Implementation Guides.
- Change the meaning or intent of any implementation specifications in the standard Implementation Guides.

Section 1.04 TennCare Introduction

TennCare is pleased to make available our Health Insurance Portability and Accountability Act (HIPAA) Companion Guide. These documents were the culmination of a long process and represent a significant milestone in our ongoing effort to adhere to the HIPAA transaction set requirements. HIPAA provides all healthcare entities a tremendous opportunity to realize many administrative and systemic benefits because it provides national standards of transaction and code sets for the electronic exchange of healthcare information. TennCare is committed to the implementation of all needed HIPAA transaction sets within the TennCare Management Information System (TCMIS).

The purpose of this manual and the accompanying documents is to provide information necessary to submit fee-for-service claims and encounters to TennCare electronically. This manual is to be used in conjunction with the National Electronic Data Interchange Transaction Set Implementation Guides. The Implementation Guides can be obtained exclusively from the Washington Publishing Company by calling 1-800-972-4334 or are available for download on their web site at www.wpc-edi.com/hipaa. IGs provide the majority of the HIPAA transaction and code set requirements, compared to TCCGs, which only provide the supplemental requirements specific to TennCare, as permitted within the structure of the HIPAA transaction sets. All clearinghouses, providers and MCCs who submit transactions electronically to TennCare must adhere to the HIPAA IGs and TCCGs requirements.

TennCare implemented HIPAA transactions on October 16, 2003. Updates to TCCG documents are provided as they are developed. Initial versions of TCCGs were posted in September 2003. *Current* TCCGs use the approved 4010 Addenda. Additional changes may be required to bring TCCGs in line with our business needs or new HIPAA IGs. The underlying point is the TCCG documents are subject to change.

HIPAA does not mandate the use of these transaction sets for the exchange of healthcare data except for certain Medicaid claims. Any provider may continue to submit paper claims and receive a paper remittance advice. However, if a provider elects to submit claims electronically and/or receive an electronic remittance advice, HIPAA does require the use of standard transactions and code sets.

All comments, suggestions, and/or questions regarding TCCGs should be directed to:

TennCare HIPAA EDI Manager
Bureau of TennCare
310 Great Circle Road
Nashville, TN 37243
Email: TennCare.EDI@state.tn.us

Submitters are requested to refrain from contacting our facility manager regarding any HIPAA issues and questions at this time.

Section 1.05 Intended Users

TCCGs are intended for the technical staff of the external entities that will be responsible for the electronic transaction/file exchanges. TCCGs are available to external entities (health plans, program contractors, providers, other state agencies, third party processors, and billing services) to clarify the information on HIPAA-compliant electronic interfaces with TennCare.

Section 1.06 HIPAA Overview

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) requires the Department of Health and Human Services to establish national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. HIPAA also addresses the security and privacy of health data. Adopting standards will eventually improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in healthcare. The intent of the law is that all electronic transactions, for which standards are specified, must be conducted according to the standards. These standards are not imposed by the law, but instead are developed by a process that included significant public and private sector input. Covered entities are required to accept these transmissions in the standard format in which they are sent and must not delay a transaction or adversely affect an entity that wants to conduct the transactions electronically.

Section 1.07 HIPAA Background

In the early 1990s, the first Bush Administration assembled an advisory group of healthcare industry leaders to discuss ways to reduce health care administrative costs across the nation. This group, which is now recognized as the Workgroup for Electronic Data Interchange (WEDI), recommended that Federal legislation be passed to implement nationwide standards of transaction and code sets to be used by the healthcare industry. This law was entitled "The Health Insurance Portability and Accountability Act" and was enacted on August 21, 1996 under the Clinton Administration.

HIPAA requires several provisions. One provision, already in effect, deals with the portability of health insurance coverage during a change in employment, and primarily affects employers and health insurers. Another provision, often referred to as "Administrative Simplification", deals with the implementation of healthcare standards, of which transaction and code sets are but one part. The following HIPAA transaction sets are currently supported by TennCare:

(a) Eligibility Inquiry and Response: HIPAA mandates X12 Version 4010A1 of the 270/271 Eligibility and Benefit Inquiry and Response EDI Transactions for this purpose.

(b) Claim Status Inquiry and Response: HIPAA mandates X12 Version 4010A1 of the 276/277 Claim Status Inquiry and Response EDI Transaction for this purpose.

(c) Referral Certification and Authorization: HIPAA mandates X12 Version 4010A1 of the 278 Health Care Service Review EDI Transaction for this purpose.

(d) Premium Payment and Remittance Advice: HIPAA mandates X12 Version 4010A1 of the 820 Group Premium Payment EDI Transaction for this purpose.

(e) Enrollment and Disenrollment: HIPAA mandates X12 Version 4010A1 of the 834 Benefit Enrollment and Maintenance EDI Transaction for this purpose.

(f) Claim Payment and Remittance Advice: HIPAA mandates X12 Version 4010A1 of the 835 Healthcare Claim Payment/Advice EDI Transaction for this purpose.

(g) Claims and Encounters: HIPAA mandates the X12 Version 4010A1 of the 837I for Institutional transactions, 837D for Dental transactions, and 837P for Professional transactions. HIPAA mandates NCPDP 5.1 for interactive pharmacy transactions and NCPDP 1.1 for pharmacy batch transactions.

Claim attachments and updates for all transaction sets are actively being developed by standards workgroups for future implementation.

HIPAA also requires the standardization of code sets. Any coded field or data element contained in a HIPAA transaction must adhere to a national set of code set values, including medical services and diagnoses. As such, TennCare required the discontinuation of local codes, most notably the Level III HCPCS (procedure codes), which were specific to TennCare. TennCare currently only uses standard code set values.

Section 1.08 Additional HIPAA Requirements

In addition to the transaction and code set aspects, there are other requirements of the "Administrative Simplification" provision of HIPAA:

(a) Privacy: Standards must be adopted by all health plans, clearinghouses, and providers that ensure the protection and appropriate disclosure of individually identifiable health information. The final rule had a mandatory implementation of April 14, 2003.

(b) Security: Standards must be adopted by all health plans, clearinghouses, and providers that ensure the integrity and confidentiality of healthcare information. The security rule addresses healthcare information in all types of media instead of just electronic format. The final rule had an implementation date of April 2005.

(c) National Identifier Codes: Standards must be adopted by all health plans, clearinghouses, and providers regarding unique identifiers for providers, plans, employers, and individuals (beneficiaries). Presently, a final rule has been issued for the Employer ID. The Department of Health and Human Services has not published final rules for the remaining identifiers.

(d) Enforcement: The Office of Civil Rights was appointed to enforce the privacy rule and has been given the authority to levy penalties for compliance failures. CMS was designated to monitor the transaction and code sets compliance.

Although TCCGs deal with only one aspect of the entire "Administrative Simplification" provision, it is worth noting that all covered entities (health plans, clearinghouses, and providers) and their business partners are required to adhere to all aspects of the provision.

Section 1.09 HIPAA Internet Links

The following is a list of government agencies, industry leaders, and transaction and code set standards organizations associated with HIPAA. This is not an exhaustive list; however, each entity plays an integral role in the success of HIPAA and collectively, represents a wealth of information that could not otherwise be included in TCCGs.

Accredited Standards Committee (ASC X12) - ASC X12 develops and maintains standards for inter-industry electronic interchange of business transactions.
http://www.x12.org/

American Dental Association (ADA) - The Dental Terminology 4th Edition codes (CDT-4, HCPCS Level II "D" codes) and the Dental Content Committee that sets standards for the dental claim form and maintains dental codes can be linked from this site.
http://www.ada.org

American Hospital Association Central Office on ICD-9-CM (AHA) - This site links to the International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM) codes, used in medical transcription and billing, and for Level I HCPCS.
www.ahacentraloffice.org

American Medical Association (AMA) - AMA owns the copyrights of the Current

Procedural Terminology 4th Edition codes (CPT-4). http://www.ama-assn.org

Association for Electronic Health Care Transactions (AFEHCT) - A healthcare association dedicated to promoting the interchange of electronic healthcare information. http://www.afehct.org

Centers for Medicare and Medicaid Services (CMS) - Formerly known as HCFA, this site provides links to multiple web sites. The Electronic Health Care Transactions and Code Sets Model Compliance Plan. The Healthcare Common Procedure Coding System (HCPCS). http://cms.hhs.gov/medicare/hcpcs For Medicaid HIPAA information related to the Administrative Simplification provision. http://www.cms.gov/medicaid/hipaa/adminsim For HIPAA administrative simplification questions, CMS maintains an e-mail address at askhipaa@cms.hhs.gov and a toll free number at (866) 282-0659.

Designated Standard Maintenance Organizations (DSMO) - This site is a resource for information about the standard setting organizations, and transaction change request system. http://www.hipaa-dsmo.org

Health Level Seven (HL7) - HL7 is one of several ANSI accredited Standards Development Organizations (SDO), and is responsible for clinical and administrative data standards. http://www.hl7.org

National Council of Prescription Drug Programs (NCPDP) - NCPDP is the standards and codes development organization for pharmacy. http://www.ncpdp.org

National Uniform Billing Committee (NUBC) - NUCB is affiliated with the American Hospital Association, and develops standards for institutional claims. http://www.nubc.org

National Uniform Claim Committee (NUCC) - NUCC is affiliated with the American Medical Association. It develops and maintains a standardized data set for use by the non-institutional health care organizations to transmit claims and encounter information. NUCC maintains the national provider taxonomy. http://www.nucc.org

Office for Civil Rights (OCR) - OCR is the Health and Human Services Office responsible for enforcing the Privacy Rule under HIPAA. http://www.hhs.gov/ocr/hipaa For HIPAA privacy questions, OCR can be contacted at OCRPrivacy@hhs.gov or by calling (866) 627-7748.

United States Department of Health and Human Services (DHHS) - This site is a resource for the Notice of Proposed Rule Making, rules and other information regarding HIPAA. http://aspe.hhs.gov/admnsimp

Washington Publishing Company (WPC) - WPC is the official publisher for HIPAA transaction implementation guides and code sets. http://www.wpc-edi.com/hipaa

Workgroup for Electronic Data Interchange (WEDI) - A workgroup dedicated to improving healthcare through electronic commerce, which includes the Strategic National Implementation Process (SNIP) for complying with the administrative simplification provisions of HIPAA. http://www.wedi.org

Article II. HIPAA Certification

Section 2.01 Certification Test Types

TennCare requires each prospective electronic data interchange (EDI) submitter to be tested and approved before HIPAA transactions will be processed in production. The Workgroup for Electronic Data Interchange (WEDI), through a collaborative healthcare industry effort called the Strategic National Implementation Process (SNIP), has recommended seven types of transaction testing:

1) Integrity Test: Testing of the EDI file for valid segments, segment order, element attributes, testing for numeric values in numeric data elements, validation of X12 syntax, and compliance with X12 rules. This will validate the basic level integrity of the EDI submission.

2) Requirement Test: Testing for HIPAA Implementation Guide-specific syntax requirements, such as repeat counts, used and not used codes, elements and segments, required or intra-segment situational data elements. Testing for non-medical code sets as laid out in the implementation guide. Values noted in the implementation guide via an X12 code list or table.

3) Balance Test: Testing the transaction for balanced field totals, financial balancing of claims or remittance advice, and balancing of summary fields, if appropriate.

4) Situational Test: Testing of specific inter-segment situations described in the HIPAA Implementation Guide, including the validation of situational fields based on rules present in the Implementation Guide for loops, segments, and data elements.

5) External Code Set Test: Testing for valid Implementation Guide-specific code set values. This type will not only validate the code sets but also make sure the usage is appropriate for any particular transaction.

6) Specialty of Line of Business Test: Testing to ensure that the segments and data elements required for certain healthcare services are present and correctly formatted according to the Implementation Guide.

7) Trading Partner Requirements Test: Testing to ensure that trading partner specific requirements are implemented.

Section 2.02 Certification Requirements

TennCare will follow the WEDI/SNIP guidelines and require each prospective EDI submitter to certify their capability to produce transactions for the top six SNIP types of transaction testing. This certification must be obtained from a third party vendor (a list of known vendors is provided later in this section). TennCare obtained a third-party certification of our capability to produce compliant transactions. It is worth noting that some vendors have added the seventh SNIP type of testing that ensures the segments and data element requirements, specific to a trading partner (such as TennCare) are present and correctly formatted. TennCare will share TCCGs with any vendor willing to offer this seventh SNIP type of testing. Although TennCare does not require certification of the seventh type at this time, it is definitely a benefit a submitter should consider when selecting a vendor for certification.

Certification for TennCare is only required for the transactions that an organization is required or plans to conduct with TennCare. Separate certification as appropriate will be required for the 837 Institutional, 837 Dental, and 837 Professional transaction sets. If your organization only does one type of 837 transactions then certification for that transaction type, not all 837 transactions, is required. TennCare is not interested in certification on transactions that are not appropriate for the Business Associate relationship. Once a certification is validated, the submitter is ready for SNIP type 7 testing and afterwards can be placed into production.

Section 2.03 Certification Vendors

As of the publication of this document, TennCare is aware of the following vendors that offer HIPAA certification services:

Company; Internet Address; Telephone; Email Address

(a) AppLabs Technologies; www.applabs.com; (215) 569-9976; info@applabs.net

(b) Claredi; www.claredi.com; (801) 444-0339; info@claredi.com

(c) Edifecs HIPAA-Desk; www.hipaadesk.com; (425) 250-0106; sales@edifecs.com

(d) HIPAA Testing; www.hipaatesting.com; (480) 946-7200; info@hipaatesting.com

A submitter is not limited to these vendors in order to obtain the required certification. Some translator vendors offer software that provides a third party certification. However, a submitter must be careful to select a vendor that offers a certification service, and not select a vendor that is limited to testing and validation services only. In addition, it is important that the vendor provide a certification for at least the top six SNIP types of transaction testing as previously discussed.

Article III. Trading Partner Agreement

Section 3.01 General Overview

Each electronic submitter will be required to complete a trading partner agreement (TPA). The TPA will be used to approve submitter identification information that is required on the HIPAA transactions. The first section of the TPA contains all of the HIPAA legal requirements. The next sections are forms used to specify transaction and security arrangements.

Two copies of a completed TPA must be mailed to TennCare at the following address:

TennCare HIPAA Project Manager
Bureau of TennCare
310 Great Circle Road
Nashville, TN 37243
Email: TennCare.EDI@state.tn.us

After the TPA is reviewed, it will be signed and one copy returned to the originator.

A WEDI/SNIP trading partner white paper can be found at
http://www.wedi.org/snip/public/articles/trading113000.pdf

Section 3.02 TennCare Electronic Data Interchange Request Form

The TennCare Electronic Data Interchange (EDI) Request Form is part of the TPA. The EDI Request Form is completed by the entity and provides a summary of the information exchanged between the entity and TennCare. This form contains information concerning:

(a) Who is the contract entity?

(b) Who is authorized to add or change the data being provided or received or the users authorized to access the data?

(c) Who will actually submit the data, if different from the contracted entity?

(d) What type of data will be accessible to the entity (e.g., Roster files, encounter or claims files, provider reference files or electronic remittance advice data)?

(e) How the data exchange will occur (e.g. SFTP or web)?

(f) What is the entity's current user ID, if available?

(g) Which transactions will generate a functional acknowledgement from the entity?

Section 3.03 TennCare User Security Agreement

The TennCare User Security Agreement, also part of the TPA, outlines the responsibilities associated with access to TennCare data. All TennCare users in the entity authorized to access data using the connection to TennCare must sign that they understand and will comply with the listed responsibilities. SFTP users will be provided an Acceptable Use Policy (AUP) that must be signed prior to access being granted. *Entities will be held responsible for the actions of their staff.* All users are expected to and will be required to comply with all Federal law, State of Tennessee law, and TennCare policies and procedures regarding data confidentiality, privacy, security, and user access.

Article IV. Technical Environment

Section 4.01 TennCare Communications Requirements

TennCare continues to evaluate and maintain current applicable methods of communications or upgrading as required with the most current and secure methods of communicating within the TCMIS. These methods include the migration from standard File Transfer Protocols (FTP) to Secure File Transfer Protocol (SFTP), NDM (IBM's Connect Direct), and Compact Disc (CD). The primary method of connecting to the TennCare network is by going from the Internet through a Virtual Private Network (VPN) tunnel to a secure FTP server. There are two types of VPN connections available:

(a) *Software-to-Hardware*. VPN client software is installed and configured on every machine at the client that requires SFTP access.

(b) *Hardware-to-Hardware*. The client's network is interfaced with the TennCare server allowing on-demand access to the SFTP server.

Detailed VPN requirements can be obtained by contacting TennCare. In general, these requirements include network interface card or modem, working Internet connection with a firewall, and installed VPN Client Software.

Section 4.02 File Encryption Procedures

Encryption is handled automatically as part of the creation of the VPN tunnel. The VPN client software on the user's computer or system will automatically de-encrypt the data after it reaches the user's system. All files and data that pass through the VPN tunnel are encrypted using at least a 128-bit algorithm.

Section 4.03 File and Directory Naming Conventions

The directory structure and file naming standards on the SFTP server are designed to provide logical access to all files, ease troubleshooting searches, and simplify security for account set ups and maintenance. TennCare's SFTP naming conventions follow.

Filenames for most HIPAA transactions will be of the format **AAAABBBYYMMDDSS.EEE** where **AAAA** is transaction type, **BBB** is the last 3-bytes of the assigned trading partner ID number, **YYMMDD** is transmission date, **SS** is transmission sequence (starting at 01), and **EEE** is file format (zip, gz, tar, etc.). The **AAAA** values reflecting the standard transaction type being transmitted and are r270 (**r**eceive), s271 (**s**end), u271 (**u**nsolicited), r276 (**r**eceive), s277 (**s**end), r278 (**r**eceive), s820 (**s**end), r834 (**r**eceive), s834 (**s**end), s835 (**s**end), d837 (**d**ental), i837 (**i**nstitutional), p837 (**p**rofessional), r997 (TennCare inbound {receive} 997), and s997 (TennCare outbound {send} 997). For example, i837ABC09070401.zip is the first institutional 837 from trading partner ABC sent on July 4, 2009 and the file is in a zip format. For the 997 transaction, the second node contains the name of the transaction being acknowledged. For example, r997ABC09021502.r834ABC09021401.zip would be a 997 response to an 834 from trading partner ABC on February 14, 2009 that was processed on February 15, 2009.

MCC encounter transactions are named following the naming standard as established in the TennCare Encounter Claims naming standard policy. TennCare Encounter policies are available on the TennCare website in the policy section (http://tennessee.gov/tenncare/forms/encounterdatapolicyworkgroup.pdf).

Naming standards for non-X12 transmissions will be provided upon completion of the TPA. Note that TennCare expects all files to be compressed with internal filename equal to the external filename with a .txt, .dat, etc. extension.

Section 4.04 HIPAA Requirements

HIPAA standards are specified in the Implementation Guide (IG) for each transaction set and any authorized addenda. The guides include:

(a) Format and contents of interchanges and functional groups,

(b) Format and contents of the header, detailer and trailer segments specific to the transaction set,

(c) Code sets and values authorized for use in the transaction set, and

(d) Allowed exceptions to specific transaction set requirements.

Section 4.05 Multiple Transactions Within a File

TennCare does not allow multiple transaction types to be submitted within a single interchange submission (ISA-ISE). While the X12 standards allow for multiple

transaction set types such as an 837I, 837P, and 834 to be submitted within an ISA-IEA, TennCare does not support transaction bundling within a file . It is thought that this limitation provides for a "cleaner" processing environment.

Section 4.06 Size of Transmissions/Batches

Fee-For-Service transmission sizes are limited based upon the number of Segments/Records allowed by HIPAA standards. HIPAA standards for the maximum file size of each transaction set are specified in the appropriate Implementation Guide or its authorized addenda.

X12 transmission sizes are based upon TennCare file transfer limits developed during systems testing. These limits are generally larger than the recommendations in IGs. For X12 transactions (837, 834, 271U), the limit is 5,000 claim encounters/recipients per ST to SE batch. This limit is imposed due to limitations discovered within the 997 associated with 1 million or more segments within a ST to SE loop. There is no limit on the NCPDP 1.1 transaction file sizes. Due to the construct of the 820 transaction the limit is 999,999 per ST-SE in the 820.

Section 4.07 Complete Transmission Check

All transactions are checked to ensure that the transmission is complete. The transaction header and footer must balance before an ISA-IEA is processed.

Section 4.08 Balancing Data Elements

TennCare will utilize any balancing requirements that can be derived from the transaction implementation guides. All financial amount fields must be balanced at all levels available within the transaction set. The number of transactions in the header and footer must equal and be the same as the number of transactions in the file.

Article V. Testing Procedures

Section 5.01 Testing Requirements

TennCare will require internal testing with all of its trading partners before a transaction is placed into production. Any submitter is welcome to request internal testing once HIPAA certification is presented to and validated by TennCare. Many details of the internal testing process and how to notify TennCare of HIPAA certification not contained in this document are part of the TPA. TennCare offers internal testing with its MCCs as a means to test TCCG requirements. However, TennCare maintains a third-party

certification of its capability to produce compliant transactions.

TennCare reserves the right to discontinue any internal testing with any submitter if TennCare determines that errors, which should have been corrected by the submitter as part of their certification process are present. TennCare currently offers full production volume testing, as part of internal testing. Upon request, TennCare will try to make available sample transaction files. Follow the contact information in section 1.04 to request sample files.

TennCare expects each individual trading partner to be responsible for ensuring that its transactions are compliant. Compliance includes both the HIPAA mandates and TennCare Trading Partner requirements contained in the TCCGs.

Compliance testing should include the internal validation of all used transaction sets. Plus, TennCare encourages entities (requires MCCs) to use a neutral third party tool/vendor to certify that the entity can produce and accept HIPAA compliant transaction sets. This tool/vendor should provide certification through type 6 compliance testing as outlined by SNIP. The SNIP white paper on testing can be found at http://www.wedi.org/snip/public/articles/testing_whitepaper082602.pdf .

After a covered entity has type 1 through type 6 certification, TennCare and the covered entity will begin more specific transaction testing to ensure testing type 7 compliance. This type of testing will ensure that files can be passed between the TCMIS and our trading partner without truncation or distortion of the data on the file.

Specifications for type 7 testing can be found in the TCCGs and other TennCare provided documentation. Any additional specific procedures for testing will be provided to the trading partner in a stand-alone memorandum immediately prior to the start of testing for a transaction set.

Section 5.02 Test Data

TennCare believes that, where possible, using “real” data will enhance the overall value of the compliance testing process. However, if the covered entity elects to do so it must ensure that it remains in compliance with all Federal and State privacy regulations. In particular, TennCare expects that Patient Identifiable Information will be encrypted or eliminated from tests submitted to the certification testing system unless the testing system is in compliance with all HIPAA regulations concerning security, privacy, and business associate agreements.

Section 5.03 Testing Procedures

Testing procedures may be provided to the trading partner in a stand-alone memorandum immediately prior to the start of testing for a given transaction set.

Article VI. Acknowledgment Processes

Section 6.01 Overview of Acknowledgment Processes

Acknowledgment transactions let the sender know that the receiver received their transactions and that the transactions have been accepted with no errors, accepted with errors, or rejected. The two types of Acknowledgment Transactions available are the:

(a) Interchange (TA1) Acknowledgment

(b) Functional Acknowledgment Transaction Set (997).

Section 6.02 TennCare Requirements

(a) TennCare uses the 997 transaction to acknowledge all X12 files received by TennCare.

(b) TennCare requires acknowledgements to be returned from its trading partners for the 834 and 271U transaction sets. This requirement may change in the future.

(c) A trading partner may elect to send TennCare an acknowledgement on any or all addition files. These acknowledgements should be listed on the EDI Request Form.

Section 6.03 997 Functional Acknowledgment Transaction Sets

The 997 Functional Acknowledgment Transaction (997 Transaction) is designed to check each functional group in an interchange for data and syntax errors and send the results back to the sending trading partner. The 997 Transaction can accept or reject records at the functional group, transaction set, segment or data element level. The HIPAA statute and current implementation guides do not mandate the use of the 997 Transaction but recommended its usage. Characteristics of the 997 Transaction include:

(a) One 997 Transaction corresponds to one functional group in the interchange.

(b) 997 Transactions are transaction sets and thus are included in the interchange control structure (envelopes) for transmission.

(c) Many commercially available translators can automatically reconcile the 997 Transaction back to the previously sent functional group. This process allows the sending trading partner to identify any transaction sets that have not been acknowledged by the receiving trading partner.

997 Transactions should not be used to acknowledge the receipt of other 997 Transactions. Details on the format and syntax of the 997 Transactions can be found in Appendix B of the Transaction Sets Standard IGs.

Section 6.04 Rejected Transmissions and Transactions

The process for handling rejected transactions and transmissions will vary based on the error(s) causing the rejection.

(a) Interchanges or functional groups may be completely rejected for IG format violations.

(b) Individual transactions or transaction sets within a functional group/interchange can be rejected in Fee-For-Service files.

(c) Rejection of encounter data will be done at the claim level or transaction set level dependent upon the error type.

Numerous edits will be performed on each transaction processed. Each of these edits has a severity level associated with it that in conjunction with the number of errors will determine accept/reject status.

Article VII. HIPAA Glossary

See website http://www.wedi.org/public/articles/HIPAA_glossary.pdf for a glossary of common HIPAA terms.

Article VIII. Other Related Information

TennCare will also continue to produce or receive several files in the agency's proprietary format. These files include:

(a) Third Party Liability (TPL) File and the related Carrier Master File.

(b) ACCENT file from DHS.

(c) DCS Regina file.

(d) SSA File.

(e) Death File from Vital Records.

(f) Provider files.

(g) Pharmacy encounter files until a NCPDP format is created.

(h) Various roster reports from other State Agencies.

(i) Proprietary reports required from the MCCs.

(j) Proprietary data extracts required by various contracts.